



# Release Notes for the Catalyst 2900 XL and Catalyst 3500 XL Switches, Cisco IOS Release 12.0(5)WC5

---

May 2002

Cisco IOS Release 12.0(5)WC5 runs on the Catalyst 2900 series XL and Catalyst 3500 series XL switches with 8-MB CPU DRAM.



**Note**

---

This release is *not* for the Catalyst 2900 LRE XL switches. Do not install this release on the Long-Reach Ethernet (LRE) switches. For information about these switches, refer to Cisco IOS Release 12.0(5)WC4.

---



**Note**

---

This release is *not* for the Catalyst 2900 XL switches with 4-MB CPU DRAM. For information about these switches, refer to Cisco IOS Release 11.2(8.10)SA6 or earlier.

---

These release notes include important information about this release and any limitations, restrictions, and caveats that apply to it. To verify that these are the correct release notes for your switch:

- If you are installing a new switch, refer to the IOS release label on the rear panel of your switch.
- If your switch is on and running, use the **show version** user EXEC command. See the “[Determining the Switch Software Version](#)” section on page 24.
- If you are upgrading to a new release, refer to the software upgrade filename for the IOS version. Before upgrading your switch to this release, read the “[Upgrading the Switch Software](#)” section on page 22.

You can download the switch software from these sites:

- <http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml>  
(for registered Cisco.com users with a login password)
- <http://www.cisco.com/public/sw-center/sw-lan.shtml>  
(for nonregistered Cisco.com users)

This release is part of a special release of Cisco IOS software that is not released on the same 8-week maintenance cycle that is used for other platforms. As maintenance releases and future releases become available, they will be posted to Cisco.com in the Cisco IOS software area.



---

**Corporate Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

# Contents

This document has the following sections:

- “Hardware Requirements” section on page 2
- “Cluster Requirements and Guidelines” section on page 5
- “Minimum Cisco IOS Release for Major Features” section on page 7
- “New Features in this Release” section on page 9
- “Limitations and Restrictions” section on page 10
- “Open Caveats” section on page 12
- “Resolved Caveats” section on page 13
- “Important Notes” section on page 15
- “Initial Switch Configuration” section on page 17
- “Upgrading the Switch Software” section on page 22
- “Related Documentation” section on page 36
- “Obtaining Documentation” section on page 36
- “Obtaining Technical Assistance” section on page 37

## Hardware Requirements

This release supports the 8-MB Catalyst 2900 XL switches (see [Table 1](#)) and Catalyst 3500 XL switches (see [Table 2](#)).



**Note**

This release is *not* for the Catalyst 2900 LRE XL switches. Do not install this release on the Long-Reach Ethernet (LRE) switches. For information about these switches, refer to Cisco IOS Release 12.0(5)WC4.



**Note**

This release is *not* for the Catalyst 2900 XL 4-MB switches. The 4-MB models are WS-C2908-XL, WS-C2916M-XL, WS-C2924C-XL, and WS-C2924-XL. These switches can only be upgraded up to Release 11.2(8.10)SA6. To be cluster members, these switches must run Release 11.2(8.x)SA6 original edition software. To determine the switch DRAM size, enter the **show version** user EXEC command.

**Table 1 Catalyst 2900 XL Switches with 8-MB CPU DRAM**

Switch	Description
Catalyst 2912MF XL	12 100BASE-FX ports and 2 high-speed expansion slots
Catalyst 2912 XL	12 autosensing 10/100 ports
Catalyst 2924M XL	24 autosensing 10/100 ports and 2 high-speed expansion slots
Catalyst 2924M DC XL	24 autosensing 10/100 ports and 2 high-speed expansion slots (DC power)
Catalyst 2924 XL	24 autosensing 10/100 ports
Catalyst 2924C XL	22 autosensing 10/100 ports and 2 100BASE-FX ports

**Table 2 Catalyst 3500 XL Switches**

Switch	Description
Catalyst 3508G XL	8 Gigabit module slots
Catalyst 3512 XL	12 autosensing 10/100 ports and 2 Gigabit module slots
Catalyst 3524 XL	24 autosensing 10/100 ports and 2 Gigabit module slots
Catalyst 3524-PWR XL	24 autosensing 10/100 inline-power ports and 2 Gigabit module slots
Catalyst 3548 XL	48 autosensing 10/100 ports and 2 Gigabit module slots

## Software Requirements

This section describes the requirements for the system and for the Cluster Management Suite (CMS) software.

### System Requirements

These operating systems are supported for CMS management:

- Microsoft Windows 95 (Service Pack 1 required)
- Microsoft Windows 98, second edition
- Microsoft Windows NT 4.0 (Service Pack 3 or higher required)
- Microsoft Windows 2000
- Solaris 2.5.1 or higher, with the Sun-recommended patch cluster for that operating system and Motif library patch 103461-24

The minimum PC requirement is a Pentium processor running at 233 MHz with 64 MB of DRAM. The minimum UNIX workstation requirement is a Sun Ultra 1 running at 143 MHz with 64 MB of DRAM. [Table 3](#) lists the recommended platforms for using CMS.

**Table 3 Recommended Minimum Platform Configuration for Web-Based Management**

OS	Processor Speed	DRAM	Number of Colors	Resolution	Font Size
Windows NT 4.0 <sup>1</sup>	Pentium 300 MHz	128 MB	65,536	1024 x 768	Small
Solaris 2.5.1	SPARC 333 MHz	128 MB	Most colors for applications	–	Small (3)

1. Service Pack 3 or higher required

## Browser and Java Plug-In Requirements

When starting a CMS session, the switch verifies the browser version to ensure that the browser is supported. If the browser is not supported, an error message appears, and the session does not start. [Table 4](#) lists the browsers supported by CMS.

CMS requires the Java plug-ins described in the [“Installing the Required Plug-In”](#) section on page 20.

**Table 4** *Browser Requirements*

Operating System	Netscape Communicator <sup>1</sup>	Microsoft Internet Explorer
Windows 95	4.61, 4.7	5.0, or 5.5
Windows 98	– <sup>2</sup>	5.0, or 5.5
Windows NT 4.0	4.61, 4.7	5.0, or 5.5
Windows 2000	4.61, 4.7	5.0, or 5.5
Solaris 2.5.1 or higher	4.61, 4.7	– <sup>3</sup>

1. Netscape Communicator version 4.60 and 6.0 are *not* supported. (CSCdx34982)
2. CMS is not supported on machines running Windows 98 and Netscape Navigator. The workaround is to use Microsoft Internet Explorer if your operating system is Windows 98. (CSCdx4997)
3. Microsoft Internet Explorer is *not* supported on Solaris 2.5.1 or higher.



### Note

If you receive an Internet Explorer error message that the page might not display correctly because your security settings prohibit the ActiveX controls, your security settings are set too high. To lower security settings, go to **Tools > Internet Options**, and select the **Security** tab. Select the indicated **Zone**, and move the **Security Level for this Zone** slider from **High** to **Medium** (the default).

To access CMS, follow the procedures in the [“Initial Switch Configuration”](#) section on page 17.

# Cluster Requirements and Guidelines

This section describes the hardware and software requirements for clustering Catalyst desktop switches.

## Catalyst 2900 XL and Catalyst 3500 XL Switches

Some versions of switch software do not support clustering, and other versions do not support some of the features in this release. To ensure that all cluster switches are using the same software level, we recommend that you upgrade all cluster switches to the software release that supports the features that you want.

If you have a cluster with switches that are running different versions of switch software, changes on the latest release might not be reflected on switches running the older versions. For example, if you start Visual Switch Manager (VSM) on a switch running Release 11.2(8)SA6, the windows and functionality can be different from a switch running Release 12.0(5)XU or later.

[Table 5](#) describes the Catalyst 2900 XL and Catalyst 3500 XL switches supported by this release and shows which switches can be command switches. All switches can function as standalone devices.

All Catalyst 2900 XL and Catalyst 3500 XL switches running Release 12.0(5.3)WC(1) and later are cluster-capable. All Catalyst 2900 XL modules are supported in cluster configurations.

We recommend that either the command switch has the latest software version installed if there switches in the cluster with older software versions or that all switches in the same platform be upgraded to the latest software version.



**Note**

We strongly recommend that the highest-end, command-capable switch in the cluster be the command switch. If your switch cluster has Catalyst 1900, Catalyst 2820, Catalyst 2900 XL, and Catalyst 3500 XL switches, either the Catalyst 2900 XL or Catalyst 3500 XL should be the command switch.



**Note**

This release is *not* for the Catalyst 2900 LRE XL switches. For information about upgrading the Catalyst 2900 LRE XL switches, refer to Release 12.0(5)WC4.

**Table 5** Catalyst 2900 XL and Catalyst 3500 XL Switches as Cluster Members

Switch	Release 12.0(5.3)WC(1) or higher?	Command Capable?	Member Capable?
Catalyst 2900 XL (4 MB of DRAM) <sup>1</sup>	No	No	Yes
Catalyst 2900 XL (8 MB of DRAM)	Yes	Yes	Yes
Catalyst 2900 LRE XL (16 MB of DRAM)	Yes	Yes	Yes
Catalyst 3500 XL	Yes	Yes	Yes

- These switches can act as cluster members if they are running Release 11.2(8.x)SA6 original edition software. They can interoperate with this software release, but they cannot be upgraded to it.

## Catalyst 3550 Switches

Catalyst 3550 switches running Release 12.0(4)EA1 or higher can be command and member switches. For more information, refer to the documentation for the Catalyst 3550 switches.


**Note**

We strongly recommend that the highest-end, command-capable switch in the cluster be the command switch. If your switch cluster has a Catalyst 3550 switch, that switch should be the command switch.

## Catalyst 2950 Switches

Catalyst 2950 switches running Release 12.0(5)WC(1) or higher can be command and member switches. For more information, refer to the documentation for the Catalyst 2950 switches.


**Note**

We strongly recommend that the highest-end, command-capable switch in the cluster be the command switch. If your switch cluster has Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL switches, the Catalyst 2950 should be the command switch.

## Catalyst 1900 and Catalyst 2820 Switches

Table 6 lists the Catalyst 1900 and Catalyst 2820 switches and the minimum software release that they require to be cluster members. All Catalyst 2820 modules are supported in cluster configurations. For more information, refer to the documentation for the Catalyst 1900 and Catalyst 2820 switches.


**Note**

We strongly recommend that the highest-end, command-capable switch in the cluster be the command switch. If your switch cluster has Catalyst 1900, Catalyst 2820, Catalyst 2900 XL, and Catalyst 3500 XL switches, either the Catalyst 2900 XL or Catalyst 3500 XL should be the command switch.

**Table 6** Catalyst 1900 and Catalyst 2820 Switches as Cluster Members

Switch	Release 9.00 (-EN)	Member Capable?	Command Capable?
Catalyst 1900	Yes	Yes	No
Catalyst 2820	Yes	Yes	No

# Minimum Cisco IOS Release for Major Features

Table 7 lists the minimum software release required to support the major features of the Catalyst 2900 XL and Catalyst 3500 XL switches.

**Table 7** *Catalyst 2900 XL (including 2900 LRE XL) and Catalyst 3500 XL Features and the Minimum Cisco IOS Release Required*

Feature	Minimum Release Required
Port security MAC address aging	Release 12.0(5)WC5
Bridge protocol data unit (BPDU) guard	Release 12.0(5)WC5
Remote Authentication Dial-In User Service (RADIUS)	Release 12.0(5)WC5
UniDirectional Link Detection (UDLD) recovery	Release 12.0(5)WC5
Support for the Cisco Coarse Wave Division Multiplexing (CWDM) Gigabit Interface Converter (GBIC) modules	Release 12.0(5)WC5
Enhanced web-based switch management (CMS)	Release 12.0(5)WC3
MAC address notification	Release 12.0(5)WC3
Internet Group Management Protocol (IGMP) filtering	Release 12.0(5)WC3
Extended cluster member compatibility with the Catalyst 2950 and Catalyst 3550 switches	Release 12.0(5)WC(1)
Multicast VLAN Registration (MVR)	Release 12.0(5)WC(1)
Cross-stack UplinkFast	Release 12.0(5)XW
Dynamic Host Configuration Protocol (DHCP)-based autoconfiguration	Release 12.0(5)XW
Support for the single-port 1000BASE-T GBIC module (WS-G5482)	Release 12.0(5)XW
WS-C3524-PWR XL switch with 10/100 inline-power ports	Release 12.0(5)XU
WS-C2924M-XL-EN-DC switch with DC power connector	Release 12.0(5)XU
WS-X2932-XL Catalyst 2900 XL 1-port 1000BASE-T module	Release 12.0(5)XU
Hot Standby Router Protocol (HSRP) for clustering	Release 12.0(5)XU
Extended discovery of cluster candidates up to 7 hops from the command switch	Release 12.0(5)XU
Support for up to 16 switches in a cluster	Release 12.0(5)XU
VLAN Trunking Protocol (VTP) pruning	Release 12.0(5)XU
Change management Virtual LAN (VLAN) for a cluster	Release 12.0(5)XU
Private VLAN edge support	Release 12.0(5)XU
UDLD for detecting unidirectional links	Release 12.0(5)XU
Extended cluster member functionality for Catalyst 1900 and 2820 switches	Release 12.0(5)XP
Remote monitoring (RMON) support through the command-line interface (CLI) or Simple Network Management Protocol (SNMP)	Release 12.0(5)XP
Change management VLAN	Release 12.0(5)XP
Quality of service (QoS) based on IEEE 802.1P class of service (CoS) values	Release 12.0(5)XP
WS-C3548-XL switch with 48 10/100 ports	Release 12.0(5)XP
WS-X2931-XL Catalyst GigaStack GBIC module	Release 12.0(5)XP

**Table 7 Catalyst 2900 XL (including 2900 LRE XL) and Catalyst 3500 XL Features and the Minimum Cisco IOS Release Required (continued)**

<b>Feature</b>	<b>Minimum Release Required</b>
Catalyst 3500 series XL switches (except WS-C3548-XL)	Release 11.2(8)SA6
Cluster management	Release 11.2(8)SA6
Terminal Access Control Access System Plus (TACACS+)	Release 11.2(8)SA6 (Enterprise Edition Software)
Network Time Protocol (NTP)	Release 11.2(8)SA6
Spanning Tree Protocol (STP) UplinkFast	Release 11.2(8)SA6 (Enterprise Edition Software)
250 VLANs (some models: see the <a href="#">“Limitations and Restrictions”</a> section on page 10)	Release 11.2(8)SA6
Catalyst 2900 series XL 1000BASE-X modules	Release 11.2(8)SA5
Catalyst 2900 series XL asynchronous transmission mode (ATM) modules	Release 11.2(8)SA5
IEEE 802.1Q trunking	Release 11.2(8)SA5 (Enterprise Edition Software)
Inter-Switch Link (ISL) trunking	Release 11.2(8)SA4 (Enterprise Edition Software)
VLAN Membership Policy Server (VMPS)	Release 11.2(8)SA4 (Enterprise Edition Software)
8192 media access control (MAC) addresses on modular switches	Release 11.2(8)SA4
Switch Network View stack management	Release 11.2(8)SA3
Web-based switch management	Release 11.2(8)SA
Fast EtherChannel port groups	Release 11.2(8)SA

# New Features in this Release

This section describes the new features in this release.

## New Hardware Support

Release 12.0(5)WC5 supports the Coarse Wave Division Multiplexing (CWDM) Gigabit Interface Converter (GBIC) modules.

## New Software Support

This section describes the new software features in this release.

### Port Security MAC Address Aging

You can use port security aging to configure dynamic source MAC addresses that the switch learns and then drops when they are not in use. The aging time parameter defines how long the switch retains unseen addresses in the MAC address table.

### BPDU Guard

The bridge protocol data unit (BPDU) guard feature shuts down Port Fast-enabled interfaces that receive BPDUs rather than putting the interfaces into the blocking state. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back in service.

### RADIUS Authentication Support

Remote Authentication Dial-In User Service (RADIUS) secures networks against unauthorized access. RADIUS clients run on supported Cisco routers and switches and send authentication requests to a central RADIUS server, which contains all user authentication and network service access information.

### UDLD Errdisable Enhancement

You can use the UniDirectional Link Detection (UDLD) Errdisable Enhancement to configure a timeout period for error-disabled ports, after which the ports are re-enabled automatically. This eliminates the need to manually re-enable all the ports. This errdisable and re-enable cycle continues until the error condition is gone.

## Limitations and Restrictions

You should review this section before you begin working with the switches. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

- All Catalyst 3500 series XL and most Catalyst 2900 series XL switches support a total of 250 VLANs and 64 spanning-tree instances. The Catalyst 2912 XL, 2924 XL, and 2924C XL switches support a total of 64 VLANs and 64 spanning-tree instances. Regardless of the switch model, only 64 spanning-tree instances are supported.
- The Cisco RPS 300 Redundant Power System (RPS) supports the Catalyst 3524-PWR XL switch. When the RPS LED on the switch is amber, the RPS is connected but down. However, this might merely mean that the RPS is in standby mode. Press **Standby/Active** on the RPS to put it into active mode. Refer to the *RPS 300 Hardware Installation Guide* for more information. You can view the RPS status by using the **show rps** privileged EXEC command.
- When connecting to the Catalyst 3524-PWR XL 10/100 inline-power ports, observe this caution:



### Caution

A Catalyst 3524-PWR XL 10/100 port needs up to 10 seconds to initially detect, power, and link to a Cisco IP Phone. If you disconnect the Cisco IP Phone before link has been established, you must wait 10 seconds before connecting another network device (other than another Cisco IP phone) to that switch port. Failing to do so can damage that network device.

---

- You can connect the switch to a PC by using the switch console port and the supplied rollover cable and the DB-9 adapter. You need to provide a RJ-45-to-DB-25 female DTE adapter if you want to connect the switch console port to a terminal. You can order a kit (part number ACS-DSBUASYN=) with this RJ-45-to-DB-25 female DTE adapter from Cisco.
- Certain combinations of port features create configuration conflicts. Refer to the “Avoiding Configuration Conflicts” section in the “Troubleshooting” chapter of the switch software configuration guide for a table that defines these conflicts.
- When you add a VTP client, follow this caution and procedure:



### Caution

Before adding a VTP client to a VTP domain, always verify that its VTP configuration revision number is *lower* than the configuration revision number of the other switches in the VTP domain. If necessary, reset the switch configuration revision number to 0. Switches in a VTP domain always use the VLAN configuration of the switch with the highest VTP configuration revision number. If you add a switch that has a revision number higher than the revision number in the VTP domain, it can erase all VLAN information from the VTP server and VTP domain.

---

Beginning in user EXEC mode, follow these steps to verify and reset the VTP configuration revision number on a switch *before* adding it to a VTP domain.

	Command	Purpose
Step 1	show vtp status	Check the VTP configuration revision number. If the number is 0, add the switch to the VTP domain. If the number is greater than 0, follow these steps: <ol style="list-style-type: none"> <li>a. Write down the domain name.</li> <li>b. Write down the configuration revision number.</li> <li>c. Continue with the next steps to reset the configuration revision number on the switch.</li> </ol>
Step 2	enable	Enter privileged EXEC mode.
Step 3	vlan database	Enter VLAN database mode.
Step 4	vtp domain <i>domain-name</i>	Change the domain name from the original one displayed in Step 1 to a new name.
Step 5	exit	The VLAN information on the switch is updated and the configuration revision number is reset to 0. You return to privileged EXEC mode.
Step 6	show vtp status	Verify that the configuration revision number has been reset to 0.
Step 7	vlan database	Enter VLAN database mode.
Step 8	vtp domain <i>domain-name</i>	Enter the original domain name on the switch.
Step 9	exit	The VLAN information on the switch is updated, and you return to privileged EXEC mode.
Step 10	show vtp status	(Optional) Verify that the domain name is the same as in Step 1 and that the configuration revision number is 0.

After resetting the configuration revision number, add the switch to the VTP domain.



#### Note

You can use the **vtp transparent** vlan database command to disable VTP on the switch and then change its VLAN information without affecting the other switches in the VTP domain. For more information about using vtp transparent mode, refer to the switch software configuration guide.

- Host names and Domain Name System (DNS) server names that contain commas on a cluster command switch, member switch, or candidate switch can cause CMS to behave unexpectedly. You can avoid this instability in the interface by not using commas in host names or DNS names. Do not use commas when also entering multiple DNS names in the Device Configuration tab (**Administration > IP Addresses**) in CMS.
- The range of seconds for the **span-tree max-age** global configuration command is now 6 to 200 seconds. If you had used this command in Release 11.2(8)SA6 or earlier to set a value greater than this range and now upgrade your software to Release 11.2(8.1)SA6 or later, the switch sets this value to the default: 20 seconds for IEEE STP and 10 seconds for IBM STP.

- When using the SPAN feature, the monitoring port receives copies of sent and received traffic for all monitored ports. If the monitoring port is 50 percent oversubscribed for a sustained period of time, it will probably become congested. One or more of the ports being monitored might also experience a slowdown.
- When using the Software Image Management (SWIM) application in the Resource Manager Essentials (RME) suite of the CiscoWorks2000 product family to perform automated system software and boot loader upgrades, you should note the following:
  - Catalyst 2900 series XL switches require Release 11.2(8)SA4 or later and RME version 2.1 or 2.2.
  - Catalyst 3500 series XL switches require Release 11.2(8.1)SA6 or later and RME version 2.2.

## Open Caveats

These are the open caveats in this release:

[“Open IOS Caveats” section on page 12](#)

[“Open CMS Caveats” section on page 13](#)

## Open IOS Caveats

These are the severity 3 IOS configuration caveats:

- CSCdv50479  
A switch that is running cross-stack UplinkFast cannot undergo a fast transition and must use the usual slow spanning tree transition stages.  
There is no workaround.
- CSCdv80043  
When you are using a terminal program to Telnet from a PC into the console port of a switch, and TACACS+ is running on that PC, the switch fails, and you lose your Telnet connection when you enter switch commands from the PC.  
The workaround is to run TACACS+ on a terminal server instead of on the PC.
- CSCdx58917  
A switch that is running Release 12.0(5)WC3b and is configured as a cluster commander does not display correct SNMP port information about cluster members.  
The workaround is to downgrade the cluster commander to Release 12.0(5)WC3. Other switches in the cluster can continue running Release 12.0(5)WC3b.

## Open CMS Caveats

These are the severity 3 CMS configuration caveats:

- CSCdx49978  
CMS does not work reliably on machines running Windows 98 and Netscape Navigator.  
The workaround is to use Microsoft Internet Explorer.
- CSCdv88724  
If a switch is running CMS for 2 to 3 days, and the switch is low on memory, the switch fails with an out of memory error.  
The workaround is to close the browser and relaunch CMS.
- CSCdx34982  
CMS does not support Netscape Navigator 6.0.  
The workaround is to use a supported version of Netscape Navigator.

## Resolved Caveats

These caveats were resolved in this release:

- [“Resolved IOS Caveats” section on page 13](#)
- [“Resolved Cluster Configuration Caveat” section on page 15](#)
- [“Resolved CMS Caveat” section on page 15](#)

## Resolved IOS Caveats

These IOS caveats were resolved in this release:

- CSCdp57240  
When a GigaStack GBIC module is inserted into the GBIC slot of a switch, the switch no longer displays a value of 1, which is the value for *not specified*.
- CSCdv87921  
After disconnecting and reconnecting the console rollover cable, the console session no longer freezes.
- CSCdw11545  
You can now set the Spanning Tree Protocol (STP) priority to 32768 when cross-stack UplinkFast is enabled.
- CSCdw42017  
When a switch is configured as a cluster commander and it does not have the address for an outgoing packet in its MAC address table, it now sends the packet out the default gateway instead of sending an ARP request for a nonlocal address.

- CSCdw42773  
When there are two uplinks to a switch and the root port and nonroot port are sequentially brought down, the other uplink that is in the blocking state no longer takes more than 10 seconds to go into the learning state.
- CSCdw59208  
When you are connected through a Telnet session and enter a **show USER** exec command that causes many pages of output to display, holding the space bar down does not halt the session.
- CSCdw80531  
When you shut down one Fast EtherChannel (FEC) port, the other ports also shut down.
- CSCdw82402  
Recovery when power cycling a root switch when running cross-stack UplinkFast is not going to go through faster convergence.
- CSCdw85801  
It is no longer necessary to disable SNMP in order to receive a ping response from the switch.
- CSCdx00341  
It is no longer necessary to enable STP to return the correct MAC address in the dot1dBaseBridgeAddress MIB variable.
- CSCdx04134  
Release 12.0(5)WC5 supports the Coarse Wave Division Multiplexing (CWDM) Gigabit Interface Converter (GBIC) modules.
- CSCdx09751  
You can use the UniDirectional Link Detection (UDLD) errdisable enhancement to configure a timeout period for error-disabled ports. After the timeout period, the ports are automatically re-enabled.
- CSCdx16308  
When you have multiple VLANs configured, you no longer need to reload a switch to reconnect the first VLAN in the list.
- CSCdx26563  
A switch no longer fails when trying to collect or send authentication, authorization, and accounting (AAA) data.
- CSCdx43881  
Entering this sequence no longer causes a switch to reload:  

```
switch(config)#aaa new-model
switch(config)#aaa group server tacacs+ test1
switch(config-sg-tacacs+)#exit
switch(config)#aaa group server radius test2
switch(config)#aaa group server radius test1
```
- CSCdx43948  
A switch no longer fails when an extended ping operation is used with the `loose` and `strict` options enabled.

## Resolved Cluster Configuration Caveat

This cluster caveat was resolved in this release:

- CSCdw66592  
Switch cluster members now provide reliable SNMP information from Cisco Building Broadband Service Manager (BBSM) products.

## Resolved CMS Caveat

No CMS caveats were resolved in this release:

## Important Notes

This section describes important information related to this release.

- The **cluster setup** privileged EXEC command was removed in Release 12.0(5)WC5.
- When you are configuring a cascaded stack of Catalyst 3500 XL switches by using a GigaStack GBIC module and want to include more than one VLAN in the stack, be sure to configure all the GigaStack GBIC interfaces as trunk ports by using the **switchport mode trunk** interface configuration command and to use the same encapsulation method by using the **switchport encapsulation {isl | dot1q}** interface configuration command. For more information about these commands, refer to the switch command reference.
- The MVR threshold feature was removed in Release 12.0(5.3)WC(1). To limit rates, use the port multicast storm control feature instead of the MVR threshold feature.

## Documentation Notes

- This information is now only in the release notes and is no longer in the manuals:
  - Hardware, software, and cluster requirements
  - Procedures for initial switch configuration: using the setup program, installing browser plug-ins, and accessing CMS
  - Procedures for upgrading the switch software
- The Catalyst 3508 XL switch (WS-C3508G-XL) ships with a power rating of 1.5A/0.75A. The back-panel illustration of the Catalyst 3508 XL switch in the *Catalyst 3500 Series XL Hardware Installation Guide* shows an outdated power rating of 1A/0.5A.
- The maximum power consumption of the Catalyst 3548 XL switch (WS-C3548-XL) is 341 Btus per hour. The *Catalyst 3500 Series XL Hardware Installation Guide* lists an incorrect value of 600 Btus per hour.

- These EMC regulatory statements are not included in the *Catalyst 3500 Series XL Hardware Installation Guide*:

## Japan

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

46464

## Korea



Warning

**This is a Class A Device and is registered for EMC requirements for industrial use. The seller or buyer should be aware of this. If this type was sold or purchased by mistake, it should be replaced with a residential-use type.**

주의 A급 기기 이 기기는 업무용으로 전자파 적합 등록을 한 기기이  
오니 판매자 또는 사용자는 이 점을 주의하시기 바라며 만약  
잘못 판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

## Hungary

This equipment is a Class A product and should be used and installed properly according to the Hungarian EMC Class A requirements (MSZEN55022). Class A equipment is designed for typical commercial establishments for which special conditions of installation and protection distance are used.

Figyelmeztetés a felhasználói kézikönyv számára:

Ez a berendezés "A" osztályú termék, felhasználására és üzembe helyezésére a magyar EMC "A" osztályú követelményeknek (MSZ EN 55022) megfelelően kerülhet sor, illetve ezen "A" osztályú berendezések csak megfelelő kereskedelmi forrásból származhatnak, amelyek biztosítják a megfelelő speciális üzembe helyezési körülményeket és biztonságos üzemelési távolságok alkalmazását.

# Initial Switch Configuration

This section provides these procedures:

- [“Using the Setup Program” section on page 17](#)
- [“Installing the Required Plug-In” section on page 20](#)
- [“Displaying the CMS Access Page” section on page 21](#)

This section assumes that you have already installed the switch and connected devices to it, as described in the switch hardware installation guide.

## Using the Setup Program

You can use an automatic setup program to assign switch IP information, host and cluster names, and passwords and to create a default configuration for continued operation. Later, you can use CMS or the command-line interface (CLI) to customize your configuration. To run the setup program, access the switch from the PC terminal that you connected to the console port. For information about connecting a PC or terminal to the switch console port, refer to the switch hardware installation guide.



### Note

If the switch will be a cluster member, you do not always need to assign IP information or a password, as the switch will be managed through the IP address of the command switch. If you are configuring a command switch or standalone switch, you need to assign IP information. Refer to the switch software configuration guide for more information.

The first time that you access the switch, it runs a setup program that prompts you for IP and other configuration information necessary for the switch to communicate with local routers and the Internet. This information is also required if you plan to use CMS to configure and manage the switch.

You will need the following information from your system administrator:

Switch IP address                    \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

Subnet mask (netmask)            \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

Default gateway (router)        \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

Enable secret password          \_\_\_\_\_

Use this procedure to create an initial configuration for the switch:



### Note

Be sure that the rollover cable is connecting a PC serial port to the switch console port. The data characteristics are 9600 baud, 8 data bits, 1 stop bit, and no parity. Use the supplied rollover cable and DB-9 adapter to connect a PC to the switch console port. You need to provide a RJ-45-to-DB-25 female DTE adapter if you want to connect the switch console port to a terminal. You can order a kit (part number ACS-DSBUASYN=) containing that adapter from Cisco. For console port and adapter pinout information, refer to the “Cable and Connector Specifications” appendix in the switch hardware installation guide.

At any point you can enter a question mark for help. Use Ctrl-C to stop the configuration dialog at any prompt. The default settings are in square brackets.

---

**Step 1** Enter **Y** at the first prompt.  
Continue with configuration dialog? [yes/no]: **y**

**Step 2** Enter the switch IP address, and press **Return**:  
Enter IP address: *ip\_address*

**Step 3** Enter the subnet mask, and press **Return**:  
Enter IP netmask: *ip\_netmask*

**Step 4** Enter **Y** at the next prompt to specify a default gateway (router):  
Would you like to enter a default gateway address? [yes]: **y**

**Step 5** Enter the IP address of the default gateway, and press **Return**.  
IP address of the default gateway: *ip\_address*




---

**Note** Enter a host name for the switch, and press **Return**.

---




---

**Note** On a command switch, the host name is limited to 28 characters; on a member switch to 31 characters. Do not use *-n*, where n is a number, as the last character in a host name for any switch.

---

Enter a host name: *host\_name*

**Step 6** Enter a secret password, and press **Return**.




---

**Note** The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows spaces, but ignores leading spaces.

---

Enter enable secret: *secret\_password*

**Step 7** Enter **Y** to enter a Telnet password:  
Would you like to configure a Telnet password? [yes] **y**




---

**Note** The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

---

**Step 8** Enter the Telnet password, and press **Return**:  
Enter Telnet password: *telnet\_password*

- Step 9** Enter **Y** to configure the switch as the cluster command switch. Enter **N** to configure it as a member switch or as a standalone switch.



**Note** If you enter **N**, the switch appears as a candidate switch in Cluster Builder. In this case, the message in [Step 10](#) is not displayed.

Would you like to enable as a cluster command switch? **y**

- Step 10** Assign a name to the cluster, and press **Return**.

Enter cluster name: *cls\_name*



**Note** The cluster name can be 1 to 31 alphanumeric characters, dashes, or underscores.

- Step 11** The initial configuration is displayed:

The following configuration command script was created:

```
ip subnet-zero
interface VLAN1
ip address 172.20.153.36 255.255.255.0
ip default-gateway 172.20.153.01
hostname host_name
enable secret 5 $1$M3pS$cXtAlkyR3/6Cn8/
line vty 0 15
password telnet_password
snmp community private rw
snmp community public ro
cluster enable cls_name

end
```

- Step 12** Verify that the information is correct.

- If the information is correct, enter **Y** at the prompt, and press **Return**.
- If the information is not correct, enter **N** at the prompt, press **Return**, and begin again at Step 1.

Use this configuration? [yes/no]: **y**

After you complete the setup program, the switch can use the created default configuration. If you want to change this configuration or want to perform other management tasks, use one of these tools:

- CMS from your browser (See the [“Installing the Required Plug-In”](#) section on page 20 and the [“Displaying the CMS Access Page”](#) section on page 21.)
- Command-line interface (CLI) (Refer to the switch software configuration guide.)

The switch software configuration guide provides more information about how to set a password to protect the switch against unauthorized Telnet access and how to access the switch if you forget the password.

## Installing the Required Plug-In

A Java plug-in is required for the browser to access CMS. Download and install the plug-in before you start CMS. Each platform, Windows and Solaris, supports three plug-in versions. For information on the supported plug-ins, see the “[Windows 95, Windows 98, and Windows NT 4.0, and Windows 2000 Users](#)” section on page 20 and the “[Solaris Platforms](#)” section on page 21.

You can download the recommended plug-ins from this URL:

<http://www.cisco.com/pcgi-bin/tablebuild.pl/java>



### Note

---

Uninstall older versions of Java plug-ins before installing the Java plug-in.

---

If the Java applet does not initialize after you have installed the plug-in, open the Java Plug-in Control Panel (**Start > Programs > Java Plug-in Control Panel**), and verify these settings:

In the Proxies tab, verify that the **Use browser settings** is checked and that no proxies are enabled.



### Note

---

If you are running McAfee VirusScan on Windows 2000 and the plug-in takes a long time to load, you can speed up CMS operation by disabling the VirusScan Internet Filter option, the Download Scan option, or both.

From the Start menu, disable the options by selecting **Start > Programs > Network Associates > Virus Scan Console > Configure**.

or

From the taskbar, right-click the Virus Shield icon, and in the Quick Enable menu, disable the options by deselecting **Internet Filter** or **Download Scan**.

---

### Windows 95, Windows 98, and Windows NT 4.0, and Windows 2000 Users

These Java plug-ins are supported on the Windows platform:

- Java plug-in 1.3.1
- Java plug-in 1.3.0
- Java plug-in 1.2.2\_05

You can download these plug-ins from this URL:

<http://www.cisco.com/pcgi-bin/tablebuild.pl/java>



### Note

---

If you start CMS without having installed the required Java plug-in, the browser automatically detects this. If you are using a supported Internet Explorer browser, it automatically downloads and installs the Java plug-in 1.3.1 (default). If you are using a supported Netscape browser, the browser displays a Cisco.com page that contains the Java plug-in and installation instructions. If you are using Windows 2000, Netscape Communicator might not detect the missing Java plug-in.

---

## Solaris Platforms

These Java plug-ins are supported on the Solaris platform:



### Caution

To avoid performance and compatibility issues, do not use Java plug-ins later than Java plug-in 1.3.1.

- Java plug-in 1.3.1
- Java plug-in 1.3.0
- Java plug-in 1.2.2\_07

If you have a SmartNet contract, you can download these plug-ins and instructions from this URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/java>

To install the Java plug-in, follow the instructions in the README\_FIRST.txt file.

If you do not have a SmartNet contract, download the plug-in from this URL:

<http://www.cisco.com/pcgi-bin/tablebuild.pl/java>



### Note

Uninstall older versions of the Java plug-in before installing Java plug-in JRE 1.3.1.

## Displaying the CMS Access Page

After the browser is configured, display the CMS access page:

- Step 1** Enter the switch IP address and your privilege level in the browser **Location** field (Netscape Communicator) or Address field (Microsoft Internet Explorer). For example:

```
http://10.1.126.45:184/level/14/
```

where 10.1.126.45 is the switch IP address, 184 is the HTTP port, and level/14 is the privilege level. You do not need to enter the HTTP port if the switch is using HTTP port 80 (the default) or enter the privilege level if you have read-write access to the switch (privilege level is 15).

For information about the HTTP port and privilege levels, refer to the switch software configuration guide.

- Step 2** When prompted for a username and password, enter only the switch enable password. CMS prompts you a second time for a username and password. Enter only the enable password again.

If you configure a local username and password, make sure you enable it by using the **ip http authentication** global configuration command. Enter your username and password when prompted.

- Step 3** Click **Cluster Management Suite**.

If you access CMS from a standalone or member switch, Device Manager appears. If you access CMS from a command switch, you can display the Front Panel and Topology views.

For complete information about CMS, refer to the switch software configuration guide.

# Upgrading the Switch Software

This section provides topics about upgrading the switch software:

- [“Guidelines for Upgrading Switch Software” section on page 22](#)
- [“Overview of the Switch Upgrade Process” section on page 23](#)
- [“Determining the Switch Software Version” section on page 24](#)
- [“Which Software Files to Download from Cisco.com” section on page 24](#)
- [“Downloading the New Software and TFTP Server Application to Your Management Station” section on page 25](#)
- [“Copying the Current Startup Configuration from the Switch to a PC or Server” section on page 26](#)
- [“Using CMS to Upgrade One or More Switches” section on page 26](#)
- [“Recovering from an Incomplete CMS Software Upgrade” section on page 27](#)
- [“Using the CLI to Upgrade a Catalyst 3500 XL Switch” section on page 31](#)
- [“Using the CLI to Upgrade Member Switches” section on page 34](#)



## Note

Before upgrading your switch to Release 12.0(5)WC5, read the [“Guidelines for Upgrading Switch Software” section on page 22](#) for important information.

## Guidelines for Upgrading Switch Software



## Note

This release is *not* for the Catalyst 2900 LRE XL switches. Do not install this release on the Long-Reach Ethernet (LRE) switches. For information about these switches, refer to Cisco IOS Release 12.0(5)WC4.

When upgrading the switch software, follow these rules:

- To upgrade the switch software, use the CMS procedure described in the [“Using CMS to Upgrade One or More Switches” section on page 26](#) or use the CLI procedures described in the [“Recovering from an Incomplete CMS Software Upgrade” section on page 27](#), [“Using the CLI to Upgrade a Catalyst 3500 XL Switch” section on page 31](#), or the [“Using the CLI to Upgrade Member Switches” section on page 34](#).
- If your switch is running Release 11.2(8)SA3, SA4, or SA5 (Catalyst 2900 XL only), we recommend that you upgrade the switch software by using VSM. If you are upgrading a switch running Release 11.2(8)SA6 or later to this release, we recommend that you use Cluster Manager. For CMS instructions for upgrading switch software, refer to the switch software configuration guide or the online help for that release.
- When using CMS, you cannot upgrade Catalyst 2900 XL and Catalyst 3500 XL switches at the same time. However, you can group together and upgrade Catalyst 1900 and Catalyst 2820 switches at the same time.
  - For Catalyst 2900 XL and Catalyst 3500 XL switches, enter the *image\_name.tar* filename in the New File Name field. The .tar file contains both the IOS image and the web-management code.
  - For Catalyst 1900 and Catalyst 2820 switches, enter the *image\_name.bin* filename in the New File Name field. The .bin file contains the software image and the web-management code.

- Upgrade Catalyst 1900 and Catalyst 2820 switches last. To function efficiently, these switches need to be rebooted shortly after the upgrade occurs. If you do not click **Reboot Cluster** in 30 seconds after the upgrade, the Catalyst 1900 and Catalyst 2820 switches automatically reboot.
- When using CMS to upgrade multiple switches from the Cisco TFTP server, the Cisco TFTP server application can process multiple requests and sessions. When using CMS to upgrade multiple switches from the Cisco TFTP server, you must first disable the **TFTP Show File Transfer Progress** and the **Enable Logging** options to avoid TFTP server failures. If you are performing multiple-switch upgrades with a different TFTP server, it must be capable of managing multiple requests and sessions at the same time.
- If you are using VSM to upgrade a specific switch, follow the steps in the [“Using CMS to Upgrade One or More Switches”](#) section on page 26.

## Overview of the Switch Upgrade Process

The software upgrade procedure has these major steps:

- Deciding which software files to download from Cisco.com, as described in the [“Which Software Files to Download from Cisco.com”](#) section on page 24.
- Downloading the .tar file from Cisco.com, as described in the [“Downloading the New Software and TFTP Server Application to Your Management Station”](#) section on page 25. This file contains the IOS image file, the e2rb.bin LRE firmware file, and the HTML files. From Cisco.com, you can also download a TFTP server application to copy the switch software from your PC to the switch, if necessary.

The **tar** command extracts the IOS image, the e2rb.bin LRE firmware file, and the HTML files from the .tar file during the TFTP copy to the switch.

- Copying the current startup configuration file, as described in the [“Copying the Current Startup Configuration from the Switch to a PC or Server”](#) section on page 26.

When you upgrade a switch, the switch continues to operate while the new software is copied to Flash memory. If Flash memory has enough space, the new image is copied to the selected switch but does not replace the running image until you reboot the switch.




---

**Note** If a failure occurs during the copy process, you can still reboot your switch by using the old image that is still on the switch.

---

If Flash memory does not have enough space for two images, your new image is copied over the existing one.




---

**Note** If a failure occurs while copying a new image to the switch, and the old image has already been deleted, you will need to use the XMODEM protocol to recover an image for the switch. For more information, refer to the “Recovering from Corrupted Software” section in the “Troubleshooting” chapter of the switch software configuration guide.

---

- Using CMS or the CLI to upgrade the software on your switch or switch cluster:
  - If you are using CMS to upgrade a switch, follow the steps in the [“Using CMS to Upgrade One or More Switches”](#) section on page 26.
  - If you are using the CLI to upgrade a switch, follow the steps in the [“Recovering from an Incomplete CMS Software Upgrade”](#) section on page 27, the [“Recovering from an Incomplete CMS Software Upgrade”](#) section on page 27, or the [“Using the CLI to Upgrade Member Switches”](#) section on page 34.

Features provided by the new software are not available until you reload the switch.

## Determining the Switch Software Version

The IOS image is stored as a *.bin* file in a directory that is named with the IOS release. A subdirectory contains the HTML files needed for web management. The image is stored on the system board Flash device (flash:).

You can use the **show version** user EXEC command to see the software version that is running on your switch. For example:

```
3500-239-34> show version
Cisco Internetwork Operating System Software
>IOS (tm) C3500x1 Software (C3500x1-C3H2S-M), Version 12.0(0.0.2)WC5, RELEASE SOFT)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Tue 14-May-02 12:57 by antonino
Image text-base: 0x00003000, data-base: 0x0034A3B8
```

You can also use the **dir filesystem:** privileged EXEC command to see the directory names of other software images that might be stored in Flash memory.



**Note**

You can use CMS to see the software versions that are running on all the switches in a cluster. Launch CMS, and select **Reports > Inventory**. CMS displays a window that shows the software versions for all the switches in the cluster.

## Which Software Files to Download from Cisco.com

New software releases are posted on Cisco.com and are also available through authorized resellers. From Cisco.com, you can also download a TFTP server application to copy the switch software from your PC to the switch.

[Table 8](#) describes the file extensions and what they mean for the upgrade procedure. [Table 9](#) and [Table 10](#) list the software files that you need from Cisco.com.

**Table 8** Possible Extensions for IOS Software Files

Extension	Description
.bin	The IOS image file that you can copy to the switch through TFTP.
.tar	A compacted file from which you can extract files by using the <b>tar</b> privileged EXEC command. The .tar file that you download from Cisco.com contains both the .bin and HTML (CMS) files.
<b>Note</b>	The CMS files are only available in the .tar file.

**Table 9 Catalyst 2900 XL Switch Software Files**

Filename	Description
c2900xl-c3h2s-mz.120-5.WC5.bin	IOS image-only file
c2900xl-c3h2s-tar.120-5.WC5.tar	IOS image file and HTML (CMS) files <b>Note</b> The CMS files are only available in the .tar file.

**Table 10 Catalyst 3500 XL Switch IOS Software Files**

Filename	Description
c3500XL-c3h2s-mz.120-5.WC5.bin	IOS image-only file
c3500XL-c3h2s-mz.120-5.WC5.tar	IOS image file and HTML files <b>Note</b> The CMS files are only available in the .tar file.

## Downloading the New Software and TFTP Server Application to Your Management Station

Follow these steps to download the new software and, if necessary, the TFTP server application, from Cisco.com to your management station:

- 
- Step 1** Use [Table 9](#) and [Table 10](#) to identify the files that you want to download.
- Step 2** Download the files from one of these locations:
- If you have a SmartNet support contract, go to one of these URLs, and download the appropriate files:
- <http://www.cisco.com/cgi-bin/tablebuild.pl/cat2900XL>  
<http://www.cisco.com/cgi-bin/tablebuild.pl/cat3500XL>
- If you do not have a SmartNet contract, go to one of these URLs, and download the appropriate files:
- <http://www.cisco.com/pcgi-bin/tablebuild.pl/cat2900XL>  
<http://www.cisco.com/pcgi-bin/tablebuild.pl/cat3500XL>
- Step 3** Use the CLI or CMS to perform a TFTP transfer of the file or files to the switch after you have downloaded the correct files to your PC or workstation.
- 

The readme.txt file describes how to download the TFTP server application. New features provided by the software are not available until you reload the software.

## Copying the Current Startup Configuration from the Switch to a PC or Server

When you make changes to a switch configuration, your changes become part of the running configuration. When you enter the command to save those changes to the startup configuration, the switch copies the configuration to the `config.text` file in Flash memory. To ensure that you can recreate the configuration if a switch fails, you might want to copy the `config.text` file from the switch to a PC or server.

The following procedure requires a configured TFTP server such as the Cisco TFTP server available on Cisco.com.

Beginning in privileged EXEC mode, follow these steps to copy a switch configuration file to the PC or server that has the TFTP server application:

---

**Step 1** Copy the file in Flash memory to the root directory of the TFTP server:

```
switch# copy flash:config.text tftp
```

**Step 2** Enter the IP address of the device where the TFTP server resides:

```
Address or name of remote host []? ip_address
```

**Step 3** Enter the name of the destination file (for example, `config.text`):

```
Destination filename [config.text]? yes/no
```

**Step 4** Verify the copy by displaying the contents of the root directory on the PC or server.

---

## Using CMS to Upgrade One or More Switches

You can use the Software Upgrade window in Cluster Manager to upgrade all or some of the switches in a cluster at once. Consider these conditions when doing an upgrade:

- When using CMS, you cannot upgrade Catalyst 2900 XL, Catalyst 2900 LRE XL, or Catalyst 3500 XL switches at the same time. However, you can group together and upgrade Catalyst 1900 and Catalyst 2820 switches at the same time.
  - For Catalyst 2900 XL and Catalyst 3500 XL switches, enter the `image_name.tar` filename in the New File Name field. The `.tar` file contains both the IOS image and the web-management code.
  - For Catalyst 1900 and Catalyst 2820 switches, enter the `image_name.bin` filename in the New File Name field. The `.bin` file contains the switch software image and the web-management code.
- Upgrade Catalyst 1900 and Catalyst 2820 switches last. To function efficiently, these switches need to be rebooted shortly after the upgrade occurs. If you do not click **Reboot Cluster** in 30 seconds after the upgrade, the Catalyst 1900 and Catalyst 2820 switches automatically reboot.

Follow these steps to use CMS to upgrade switch software. Refer to the online help for more details.

- 
- Step 1** In Cluster Manager, select **System > Software Upgrade** to display the Software Upgrade window.
- Step 2** Enter the .tar filename (for Catalyst 2900 XL and Catalyst 3500 XL switches) or the .bin filename (for Catalyst 1900 and Catalyst 2820 switches) that contains the IOS image and the web-management code. You can enter just the filename or a pathname into the **New Image File Names** field. You do not need to enter a pathname if the image file is in the directory that you have defined as the TFTP root directory.
- 



**Note** You can also use Cluster Manager to upgrade a single switch by following the same upgrade procedure.

---



**Note** Close your browser after the upgrade process is complete.

---

On the Catalyst 2900 XL and Catalyst 3500 XL switches, new images are copied to Flash memory and do not affect operation. The switch checks Flash memory to ensure that there is sufficient space before the upgrade takes place. If there is enough space, the new image is copied to the switch without replacing the old image, and after the new image is completely downloaded, the old one is erased. In this case, you can still reboot your switch by using the old image if a failure occurs during the copy process.

If there is not enough space in Flash memory for the new and old images, the old image is deleted, and the new image is downloaded.

On the Catalyst 1900 and Catalyst 2820 switches, the new image overwrites the current image during the upgrade.



**Note** If a failure occurs while copying a new image to the switch, and the old image has already been deleted, you need to use the XMODEM protocol to recover an image for the switch. For more information, refer to the “Recovering from Corrupted Software” section in the “Troubleshooting” chapter of the switch software configuration guide.

---

## Recovering from an Incomplete CMS Software Upgrade

An upgrade failure can create multiple copies of IOS images and other files in Flash memory. This would not leave enough space for the HTML files to also be copied to Flash memory; thus, you will not be able to access the switch through CMS.

If a failure occurs, ensure that the image file in Flash memory has the same name as the contents of the boot variable:

- See [Step 5](#) and [Step 9](#) in the “Using the CLI to Upgrade an 8-MB Catalyst 2900 XL Switch” section on [page 28](#)
- See [Step 4](#) and [Step 10](#) in the “Using the CLI to Upgrade a Catalyst 3500 XL Switch” section on [page 31](#)

If the contents of the boot variable and the image file name are the same, the switch can reset successfully. If they are different, rename the image file, or reset the boot variable by entering the **system boot name** global configuration command. The boot variable and the image file name should be the same.

To recover from the incomplete download of the HTML files, log in to the switch, and upgrade the software as described in the [“Using the CLI to Upgrade Member Switches”](#) section on [page 34](#).

## Using the CLI to Upgrade an 8-MB Catalyst 2900 XL Switch



**Caution**

The 4-MB Catalyst 2900 XL switches do not have sufficient memory to be upgraded to this release. The 4-MB models are WS-C2908-XL, WS-C2916M-XL, WS-C2924C-XL, and WS-C2924-XL. These switches must run Release 11.2(8.x)SA6 to be cluster members.

This procedure is for upgrading Catalyst 2900 XL switches with 8 MB of DRAM. You upgrade a switch by extracting the IOS image file and the HTML files from a combined .tar file. You copy the files to the switch from a TFTP server and extract the files by entering the **tar** privileged EXEC command with these results:

- Changes the name of the current image file to the name of the new file that you are copying and replaces the old image file with the new one by using the **tar privileged EXEC command**.
- Disables access to the HTML pages and deletes the existing HTML files before you upgrade the software to avoid a conflict with users accessing the web pages during the software upgrade.
- Re-enables access to the HTML pages after the upgrade is complete.

If you are unsure whether your switch has 4 MB or 8 MB of memory, you can verify memory capacity at Step 4.

Follow these steps to upgrade the switch software by using the **tar** privileged EXEC command to start a TFTP transfer:

**Step 1** If your PC or workstation cannot act as a TFTP server, copy the file to a TFTP server to which you have access.

**Step 2** Access the CLI by starting a Telnet session or by connecting to the switch console port through the RS-232 connector.

To start a Telnet session on your PC or workstation, enter this command:

```
server% telnet switch_ip_address
```

Enter the Telnet password if you are prompted to do so.

**Step 3** Enter privileged EXEC mode:

```
switch> enable
switch#
```

Enter a password if you are prompted to do so.

**Step 4** Confirm that you have an 8-MB switch:

```
switch# show version
Cisco Internetwork Operating System Software IOS (tm)
C2900XL Software (C2900XL-HS-M), Version 11.2(8.2)SA6, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1998 by cisco Systems, Inc.
Compiled Mon 23-Nov-98 20:59 by paulines
Image text-base: 0x00003000, data-base: 0x00202144
```

```
ROM: Bootstrap program is C2900XL boot loader
```

```
2900XL-EN-84.3 uptime is 1 day, 22 hours, 23 minutes
System restarted by power-on
Running default software
```

```
cisco WS-C2924-XL (PowerPC403GA) processor (revision 0x11)
with 8192K/1024K bytes of memory.
```



```
Processor board ID 0x0E, with hardware revision 0x01
Last reset from power-on
```

```
Processor is running Enterprise Edition Software
24 Ethernet/IEEE 802.3 interface(s)
```

```
32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:50:80:39:EC:40
Motherboard assembly number: 73-3382-04
Power supply part number: 34-0834-01
Motherboard serial number: FAA02499G7X
Model number: WS-C2924-XL-EN
System serial number: FAA0250U03P
Configuration register is 0xF
```

**Step 5** Display the name of the running (default) image file (BOOT path-list). This example shows the name in italic:

```
switch# show boot
→ BOOT path-list:   flash:current_image
Config file:       flash:config.text
Enable Break:      1
Manual Boot:       no
HELPER path-list:
NVRAM/Config file
buffer size: 32768
```

If there is no file defined in the BOOT path-list, enter the **dir flash:** privileged EXEC command to display the contents of Flash memory. For example, the file named *c2900XL-c3h2-mz-120-5.3.WC.1.bin* is the image file.

```
c2900XL-c3h2-mz-120-5.3.WC.1.bin
switch# dir flash:
Directory of flash:/

→  2  ---x      1644046  Apr 04 1993 15:22:13  c2900XL-c3h2s-mz-120-5.3.WC.1.bin
   4  d--x          6848  Apr 04 1993 15:23:11  html
   6  -rwx           79  Apr 04 1993 15:20:34  env_vars
   5  ---x          106  Apr 04 1993 15:20:36  info
  68  -rwx          1399  May 16 2000 14:43:42  config.text
 259  ---x           106  Apr 04 1993 15:23:12  info.ver

3612672 bytes total (940032 bytes free)
```

**Step 6** Using the exact, case-sensitive name of the combined .tar file that you downloaded, rename the running image file to that name, and replace the .tar extension with a .bin extension. The image file name is then the same as the downloaded file name but with a .bin extension. This step does not affect the operation of the switch.

```
switch# rename flash:current_image flash:new_image
Source filename [current_image]?
Destination filename [new_image]?
```

For example:

```
switch# rename flash:c2900XL-h2-mz-112.8.2-SA6.bin
flash:c2900XL--C3h2s-mz-120-5.3.WC.1.bin
Source filename [c2900XL-h2-mz-112.8.2-SA6.bin]?
Destination filename [c2900XL-c3h2s-mz-120-5.3.WC.1.bin]?
```

**Step 7** Enter global configuration mode:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

**Step 8** Disable access to the switch HTML pages:

```
switch(config)# no IP http server
```

**Step 9** If you entered the **boot** global configuration command with the name of the image file, enter this command to change the image filename to the new name.

```
switch(config)# boot system flash:new_image
```

For example:

```
switch(config)# boot system flash:c2900XL-c3h2s-mz-120-5.3.WC.1.bin
```



**Note** If the **show boot** privileged EXEC command that you entered in [Step 5](#) displays no image name, you do not need to enter this command; the switch automatically finds the correct file to use when it resets.

**Step 10** Return to privileged EXEC mode:

```
switch(config)# end
```

**Step 11** Remove the HTML files:

```
switch# delete flash:html/*
```

**Step 12** Press **Enter** to confirm the deletion of each file. Do not press any other keys during this process.

**Step 13** If upgrading from Release 11.2(8)SA5 or earlier, remove the files in the Snmp directory:

```
switch# delete flash:html/Snmp/*
```

Make sure the *S* in *Snmp* is uppercase.

Press **Enter** to confirm the deletion of each file. Do not press any other keys during this process.



**Caution**

In the following step, the **tar** privileged EXEC command copies the combined .tar file that contains both the image and the HTML files. You do not need to copy an HTML.tar file in this procedure.

**Step 14** Enter this command to copy the new image and HTML files to the switch Flash memory:

```
switch# tar /x tftp://server_ip_address/path/filename.tar flash:
Loading /path/filename.tar from server_ip_address (via VLAN1):!
extracting info (111 bytes)
extracting c2900XL-c3h2s-mz-120-5.3.WC.1.bin (1557286 bytes)!!!!!!!!!!!!!!!!!!!!!!
html/ (directory)
extracting html/Detective.html.gz (1139 bytes)!
extracting html/ieGraph.html.gz (553 bytes)
extracting html/DrawGraph.html.gz (787 bytes)!
. . .
```

Depending on the TFTP server being used, you might need to enter only one slash (/) after the *server\_ip\_address* in the **tar** privileged command.

**Step 15** Enter global configuration mode:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

**Step 16** Re-enable access to the switch HTTP pages:

```
switch(config)# IP http server
```

**Step 17** Return to privileged EXEC mode:

```
switch(config)# end
```

**Step 18** Reload the new software with this command:

```
switch# reload
System configuration has been modified. Save? [yes/no]:y
Proceed with reload? [confirm]
```

**Step 19** Press **Return** to confirm the reload.

Your Telnet session ends when the switch resets.

**Step 20** After the switch reboots, use Telnet to return to the switch, and enter the **show version** privileged EXEC command to verify the upgrade procedure. If you have a previously opened browser session to the upgraded switch, close the browser, and restart it to ensure that you are using the latest HTML files.

## Using the CLI to Upgrade a Catalyst 3500 XL Switch

This procedure is for upgrading Catalyst 3500 XL switches by copying the combined .tar file to the switch. You copy the files to the switch from a TFTP server and extract the files by entering the **tar** privileged EXEC command, with these results:

- Changes the name of the current image file to the name of the new file that you are copying and replaces the old image file with the new one.
- Disables access to the HTML pages and deletes the existing HTML files before the software upgrade to avoid a conflict if users access the web pages during the software upgrade.
- Re-enables access to the HTML pages after the upgrade is complete.

Follow these steps to upgrade the switch software by using a TFTP transfer:

**Step 1** If your PC or workstation cannot act as a TFTP server, copy the file to a TFTP server to which you have access.

**Step 2** Access the CLI by starting a Telnet session or by connecting to the switch console port through the RS-232 connector.

To start a Telnet session on your PC or workstation, enter this command:

```
server% telnet switch_ip_address
```

Enter the Telnet password if you are prompted to do so.

**Step 3** Enter privileged EXEC mode:

```
switch> enable
switch#
```

Enter the password if you are prompted to do so.

**Step 4** Display the name of the running (default) image file (BOOT path-list). This example shows the name in *italic*:

```
switch# show boot
BOOT path-list:  flash:current_image
Config file:     flash:config.text
Enable Break:    1
Manual Boot:     no
```

```
HELPER path-list:
NVRAM/Config file
buffer size: 32768
```

**Step 5** If there is no software image defined in the BOOT path-list, enter the **dir flash:** privileged EXEC command to display the contents of Flash memory.

**Step 6** Using the exact, case-sensitive name of the combined .tar file that you downloaded, rename the running image file to that name, and replace the .tar extension with .bin. The image filename is then the same as the downloaded filename but with a .bin extension. This step does not affect the operation of the switch.

```
switch# rename flash:current_image flash:new_image
Source filename [current_image]?
Destination filename [new_image]?
```

For example:

```
switch# rename flash:c3500XL-c3h2-mz-112.8.2-SA6.bin
flash:c3500XL-C3h2s-mz-120-5.3.WC.1.bin
```

**Step 7** Display the contents of Flash memory to verify the renaming of the file:

```
switch# dir flash:
Directory of flash:/

→  2  ---x   1644045  Apr 04 1993 15:17:15  c3500XL-c3h2s-mz-120-5.3.WC.1.bin
   3  -rwx     415    Jun 13 1993 05:15:37  placement.txt
   4  d--x   6848    May 03 2000 10:47:58  html
  70  -rwx     20    Mar 21 1993 09:17:03  prefs.text
   6  ---x     106    Mar 01 1993 21:56:52  info
 228  ---x     106    Apr 04 1993 15:17:54  info.ver
   69  -rwx   2188    Mar 13 1993 03:38:28  config.text
 230  -rwx     744    Mar 25 1993 19:16:46  vlan.dat
 115  -rwx     354    Mar 13 1993 04:17:15  env_vars

3612672 bytes total (936960 bytes free)
```

**Step 8** Enter global configuration mode:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

**Step 9** Disable access to the switch HTML pages:

```
switch(config)# no IP http server
```

**Step 10** Enter the **boot** global configuration command with the name of the new image filename:

```
switch(config)# boot system flash:new_image
```

For example:

```
switch(config)# boot system flash:c3500XL-C3h2S-mz-120-5.3.WC.1.bin
```



**Note** If the **show boot** privileged EXEC command in [Step 4](#) displays no image name, you do not need to enter this command; the switch automatically finds the correct file to use when it resets.

**Step 11** Return to privileged EXEC mode:

```
switch(config)# end
```

**Step 12** Remove the HTML files:

```
switch# delete flash:html/*
```

Press **Enter** to confirm the deletion of each file. Do not press any other keys during this process.



**Caution**

In the following step, the **tar** privileged EXEC command copies the combined .tar file that contains both the image and the HTML files. You do *not* need to copy an HTML .tar file in this procedure.

**Step 13** Enter this command to copy the new image and HTML files to Flash memory:

```
switch# tar /x tftp://server_ip_address/path/filename.tar flash:
Loading /path/filename.tar from server_ip_address (via VLAN1):!
extracting info (110 bytes)
extracting c3500XL-c3h2s-mz-120-5.3.WC.1.bin (1271095 bytes)!!!!!!!!!!!!!!!!!!!!!!
html/ (directory)
extracting html/Detective.html.gz (1139 bytes)!
extracting html/ieGraph.html.gz (553 bytes)
extracting html/DrawGraph.html.gz (787 bytes)
extracting html/GraphFrame.html.gz (802 bytes)!
...
```

Depending on the TFTP server being used, you might need to enter only one slash (/) after the *server\_ip\_address* in the **tar** privileged EXEC command.

**Step 14** Enter global configuration mode:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

**Step 15** Re-enable access to the switch HTTP pages:

```
switch(config)# IP http server
```

**Step 16** Return to privileged EXEC mode:

```
switch(config)# end
```

**Step 17** Reload the new software with this command:

```
switch# reload
System configuration has been modified. Save? [yes/no]:y
Proceed with reload? [confirm]
```

**Step 18** Press **Return** to confirm the reload.

Your Telnet session ends when the switch resets.

**Step 19** After the switch reboots, use Telnet to return to the switch, and enter the **show version** privileged EXEC command to verify the upgrade procedure. If you have a previously opened browser session to the upgraded switch, close the browser, and restart it to ensure that you are using the latest HTML files.

## Using the CLI to Upgrade Member Switches

Because a member switch might not be assigned an IP address, command-line software upgrades through TFTP are managed through the command switch.

This section provides these procedures:

- “Upgrading Catalyst 2900 XL or Catalyst 3500 XL Member Switches” section on page 34
- “Upgrading Catalyst 1900 or Catalyst 2820 Member Switches” section on page 35

### Upgrading Catalyst 2900 XL or Catalyst 3500 XL Member Switches

Follow these steps to upgrade the software on a Catalyst 2900 XL or Catalyst 3500 XL member switch:

**Step 1** In privileged EXEC mode on the command switch, display information about the cluster members:

```
switch# show cluster members
```

From the display, select the number of the member switch that you want to upgrade. The member number is in the SN column of the display. You need this member number for Step 2.

**Step 2** Log in to the member switch (for example, member number 1):

```
switch# rcommand 1
```

**Step 3** Start the TFTP copy function as if you were initiating it from the command switch.

```
switch-1# tar /x tftp://server_ip_address/path/filename.tar flash:
Source IP address or hostname [server_ip_address]?
Source filename [path/filename]?
Destination filename [flash:new_image]?
Loading /path/filename.bin from server_ip_address (via!)
[OK - 843975 bytes]
```

**Step 4** Reload the new software with the following command:

```
switch-1# reload
System configuration has been modified. Save? [yes/no]:y
Proceed with reload? [confirm]
```

Press **Enter** to start the download.

You lose contact with the switch while it reloads the software. For more information on the **rcommand** privileged EXEC command, refer to the switch command reference.

## Upgrading Catalyst 1900 or Catalyst 2820 Member Switches

Follow these steps to upgrade the software on a Catalyst 1900 or Catalyst 2820 member switch:

- 
- Step 1** In privileged EXEC mode on the command switch, display information about the cluster members:
- ```
switch# show cluster members
```
- From the display, select the number of the member switch that you want to upgrade. The member number is in the SN column of the display. You need this member number for Step 2.
- Step 2** Log in to the member switch (for example, member number 1):
- ```
switch# rcommand 1
```
- Step 3** For switches running standard edition software, enter the password (if prompted), access the Firmware Configuration menu from the menu console, and perform the upgrade. Follow the instructions in the installation and configuration guide that shipped with your switch. When the download is complete, the switch resets and begins using the new software.
- The Telnet session accesses the menu console (the menu-driven interface) if the command switch password is privilege level 15. If the command switch password is privilege level 1, you are prompted for the password.
- You lose contact with the switch while it reloads the software.
- Step 4** For switches running Enterprise Edition Software, start the TFTP copy as if you were initiating it from the member switch:
- ```
switch-1# copy tftp://host/src_file opcode
```
- For example, **copy tftp://spaniel/op.bin opcode** downloads new system operational code *op.bin* from the host *spaniel*.
- 

When the download is complete, the TFTP successfully downloaded operational code message appears, and the switch resets and begins using the new software.

You can also upgrade the switch software through the Firmware Configuration menu from the menu console. For more information, refer to the installation and configuration guide that shipped with your switch.

You lose contact with the switch while it reloads the software.

## Related Documentation

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the “[Ordering Documentation](#)” section on page 37.

These publications provide more information about the switches and the switch software:

- *Catalyst 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide* (order number DOC-786511=)
- *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference* (order number DOC-7812155=)
- Cluster Management Suite (CMS) online help (available only from the switch CMS software)
- *Catalyst 2900 Series XL Hardware Installation Guide* (order number DOC-786461=)
- *Catalyst 3500 Series XL Hardware Installation Guide* (order number DOC-786456=)
- *Catalyst 2900 Series XL Modules Installation Guide* (order number DOC-CAT2900-IG=)
- *Catalyst 2900 Series XL ATM Modules Installation and Configuration Guide* (order number DOC-785472=)
- *1000BASE-T Gigabit Interface Converter Installation Note* (not orderable but is available on Cisco.com)
- *Catalyst GigaStack Gigabit Interface Converter Hardware Installation Guide* (order number DOC-786460=)
- *Installation Note for the CWDM Passive Optical System* (not orderable but available on Cisco.com)

## Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

<http://www.cisco.com>

Translated documentation is available at the following URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

## Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products Marketplace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click the **Fax** or **Email** option under the “Leave Feedback” at the bottom of the Cisco Documentation home page.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems  
Attn: Document Resource Connection  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support

- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

### Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

<http://www.cisco.com/register/>

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

## Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That’s Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0203R)

Copyright © 1998-2002, Cisco Systems, Inc.  
All rights reserved.

